UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
FLORENCE DIVISION

Lisa Frierson, individually and on behalf of all others similarly situated, *Plaintiff*, v. T-Mobile US, Inc. and T-Mobile USA, Inc., *Defendants*.	**Civil Action No.** **CLASS ACTION COMPLAINT** **JURY TRIAL REQUESTED**

Plaintiff Lisa Frierson, by and through counsel, on behalf of herself and others similarly situated brings this Class Action Complaint against T-Mobile US, Inc. and T-Mobile USA, Inc. ("Defendants" or "T-Mobile"). Upon personal knowledge, investigation of counsel, and upon information and belief, Plaintiff states and alleges as follows:

PRELIMINARY STATEMENT

1. Plaintiff seeks monetary damages, restitution, and/or injunctive relief for the proposed Class and Subclass, as defined below. Plaintiff's personally-identifiable information ("PII") was exfiltrated and compromised in the data breach announced by T-Mobile on January 19, 2023 (the "Data Breach"), and Plaintiff brings this action on behalf of herself and all those similarly situated both across the United States and within her State of residence. Because only T-Mobile (and the cybercriminals who perpetrated the Data Breach) have knowledge of what

information was compromised, Plaintiff reserves her right to supplement these allegations with additional facts and injuries as they are discovered.

2. T-Mobile is one of the largest consumer brands in the United States. T-Mobile has over 100 million customers and collects immense amounts of personal identifying data related to its customers. Even with roughly 100 million paying customers, T-Mobile strives to increase its bottom line by selling this aforementioned personal identifying information. In short, T-Mobile is entrusted by millions of people with their personal communications, personal pictures, personal internet search histories, and any other function a T-Mobile smart device may have and instead of keeping this data private, T-Mobile sells it.

3. T-Mobile understood it had an enormous responsibility to protect the data it collected and assured consumers through its Privacy Policy that T-Mobile uses "administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control." Its Privacy Policy likewise acknowledges that its consumers "trust T-Mobile to connect [them] to the world every day," that "[a] big part of that is maintaining [their] privacy," and that they "deserve transparency, education, choice, protection, and simplicity."[1]

4. T-Mobile completely failed to meet these obligations and protect sensitive consumer data. Instead, even after it experienced one of the largest and most consequential data breaches in U.S. history in August 2021, T-Mobile has once again suffered a massive data breach—which is at least its eighth data breach since 2017—which compromised the highly sensitive personal information of 37 million consumers..

II. JURISDICTION AND VENUE

[1] https://www.t-mobile.com/privacy-center/privacy-notices/t-mobile-privacy-notice

5. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as Defendants are citizens of States different from that of at least one Class member.

6. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

7. This Court has personal jurisdiction over T-Mobile USA, Inc. because it is authorized to and regularly conducts business in the State of South Carolina. T-Mobile sells, markets, and advertises its products and services to Plaintiff and Class Members located in the State of South Carolina and, therefore, has sufficient minimum contacts to render the exercise of jurisdiction by this Court proper and necessary.

8. This Court has personal jurisdiction over T-Mobile US, Inc. because it is authorized to and regularly conducts business in the State of South Carolina. T-Mobile sells, markets, and advertises its products and services to Plaintiff and Class Members located in the State of South Carolina and, therefore, has sufficient minimum contacts to render the exercise of jurisdiction by this Court proper and necessary.

9. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

III. PARTIES

10. Defendant T-Mobile US, Inc. and its wholly-owned subsidiary T-Mobile USA, Inc. are telecommunications companies that provide wireless voice, messaging, and data services along

with mobile phones and accessories. T-Mobile US, Inc. and T-Mobile USA, Inc. are headquartered in Bellevue, Washington and Overland Park, Kansas in the Kansas City Metropolitan area, and is incorporated under the laws of the State of Delaware.

11. Plaintiff Lisa Frierson is a resident of the State of South Carolina and is a current customer of T-Mobile. Plaintiff has been a T-Mobile customer since July of 2017 and had no cellular data breach issues prior to switching to T-Mobile. Plaintiff Frierson has two children who are also T-Mobile customers, both of which have experienced issues since the Data Breach.

12. Plaintiff learned of the Data Breach from a news source soon after the announcement of the Data Breach on in January of 2023.

13. As a result of the Data Breach, Plaintiff spent time and effort in reviewing her CashApp, Facebook, and Instagram accounts for fraudulent activity. Also, Plaintiff spent time and effort researching the Data Breach and a possible remedy for the Data Breach. Plaintiff Frierson has noticed suspicious activity including spam calls, texts, emails, and Facebook activity.

14. Plaintiff places significant value in the security of her PII. Plaintiff entrusted her sensitive PII to T-Mobile with the understanding that T-Mobile would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

15. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury and remains at a substantial and imminent risk of future harm.

IV. FACTUAL ALLEGATIONS

A. T-Mobile Collects, Stores, and Profits from Consumer Information, and Promises to Keep it Secure.

16. T-Mobile is a U.S. wireless carrier formed in 1999 following Deutsche Telekom's purchase of VoiceStream Wireless. After the purchase, Deutsche Telekom renamed the U.S. wireless business "T-Mobile." Following a series of mergers and acquisitions—including mergers with MetroPCS in 2013 and Sprint Corporation in 2020—T-Mobile grew to the second largest wireless carrier in the United States, with over 100 million current subscribers. T-Mobile is a publicly traded company organized and operated for the profit and financial benefit of its shareholders. In 2021, T-Mobile had annual gross revenues of over $80 billion, with net income over $3 billion.

17. T-Mobile has often attempted to distinguish itself from its competitors by promoting its purportedly unique customer experience. For example, since 2013 T-Mobile has marketed itself as the "un-carrier," providing wireless services with no service contracts.[2] As current CEO Michael Sievert has described it, T-Mobile's strategy as an un-carrier means "the ability to enjoy the services we sell, like an unlimited network offering that doesn't require a contract."[3]

18. As the "uncarrier," T-Mobile offers different types of plans, including prepaid plans, wherein customers prepay for services they then receive, and postpaid plans, wherein customers can be billed for monthly services already received.[4]

19. To run its business, T-Mobile collects, maintains, and profits from the PII of millions of U.S. consumers. PII is information that is used to confirm an individual's identity and can include an individual's name, Social Security number, driver's license number, phone number,

[2] *The Un-carrier Means Business* (May 3, 2021), available at https://www.t-mobile.com/news/business/the-un-carrier-means-business.
[3] *What is an Uncarrier? We Ask T-Mobile Chief Marketing Officer Mike Sievert* (Jan. 23, 2013), available at https://www.digitaltrends.com/mobile/t-mobile-disruptive-mike-sievert/.
[4] Id.

financial information, and other identifying information unique to an individual. For T-Mobile, this information also includes unique technical identifiers tethered to customers' mobile phones. T-Mobile collects this PII from prospective and current customers and maintains and profits from the PII regardless of whether a potential customer eventually selects T-Mobile as a wireless carrier. T-Mobile also maintains the PII of former customers for an indefinite period of time.

20. T-Mobile's Privacy Policy is available on its website[5] and states that it applies "to personal data we have about you," meaning data that "identifies, relates to, describes, can be associated with, or could reasonably identify you as an individual." This includes "data like your name, address, or email address, as well as less obvious data like demographic data, device and usage data, call records, advertising ID, and location data[.]" It further states that the Notice applies to "all personal data we collect and use when you access or use our cell and data services, websites, apps, and other services (our 'services'), purchase and use our devices and products ('products'), visit our retail stores, or communicate or interact with us in any way."[6]

21. The Privacy Policy provides customers with detailed promises regarding the treatment of their PII, including how T-Mobile uses customers' data for its own benefit and profit. For example, T-Mobile confirms that it uses customers' personal data to "[a]dvertise and market products and services from T-Mobile and other companies to you, including through targeted advertising and communications about promotions and events, contents, and sweepstakes"; and to "[c]onduct research and create reports from analysis of things like usage patterns and trends and deidentify or aggregate personal data to create business and market analysis and reports."[7]

[5] https://www.t-mobile.com/privacy-center/privacy-notices/t-mobile-privacy-notice
[6] Id.
[7] Id.

22. According to the Privacy Policy's California privacy rights section, included for purposes of complying with the California Consumer Protection Act ("CCPA"), in the past 12 months T-Mobile (which also includes Sprint) has sold to third parties "device identifiers and internet and electronic network activity to facilitate online advertising. This means that a unique, resettable number that identifies your device was linked to online activity and shared with others who use that data for advertising and analytics purposes (like advertising networks, data analytics providers, and social media platforms)."[8]

23. Based on the customer PII T-Mobile collects and sells, T-Mobile states that its customers "may see T-Mobile and other advertisements on your devices, whether you're connected to our network or not. These ads may be targeted to your device based on information that we, the advertiser, and other third parties have about your behavior or interests[.]"[9]

24. T-Mobile also "works with third parties, including advertising networks, which collect information about you through devices, websites, and apps, serve ads for us and others, and measure their effectiveness..... For example, third parties like Google Ad Manager and Nielsen may use technology to collect data to deliver, personalize, and measure ads for some of our Products and Services. This technology allows tracking of device activity over time across online properties."[10]

25. In addition, T-Mobile partners "with analytic service providers like Google Analytics to help track your use of our products and services." Further: "If your mobile device is turned on, our network is collecting data about where it is. We may use, provide access to, or disclose this network location data without your permission to provide and support our services."

[8] https://www.t-mobile.com/privacy-center/privacy-notices/advertising-solutions-privacy-notice
[9] https://www.t-mobile.com/privacy-center/privacy-notices/t-mobile-privacy-notice
[10] Id.

26. T-Mobile agreed at the time of the Data Breach that it would only share data under certain enumerated circumstances, which include: "with your consent or at your direction," "with the account holder," "between T-Mobile brands and companies," "to provide benefits," "to our service providers," "to other third parties for uses described in this notice or for purposes you have requested," "for identity verification and fraud prevention services," "caller ID providers," "in a business transfer or transaction" which is specified as a "corporate business transaction like an acquisition, divestiture, sale of company assets," and "for legal process and protection." None of the enumerated circumstances involve sharing Plaintiff's or the Class Members' PII with a criminal hacker.

27. After enumerating the ways it would limit the sharing of consumer's PII and also listing the ways T-Mobile benefits and profits from tracking and targeting its customers and non-customers through collecting and maintaining their valuable PII, T-Mobile's Privacy Policy pledges to them that their PII is secure, stating that: (i) personal data will be disclosed only "with your consent, which we may get in writing, online, or orally," and (ii) T-Mobile uses "administrative, technical, contractual, and physical safeguards designed to protect your data." As discussed herein, T-Mobile failed to comply with these promises to protect Plaintiff's PII.

28. T-Mobile's acknowledges that consumers "trust T-Mobile to connect you to the world every day, and we're working hard to earn a place in your heart. A big part of that is maintaining your privacy. We believe you deserve transparency, education, choice, protection, and simplicity." These assurances have proved hollow for the millions of consumers affected by T-Mobile's breach of trust and failure to protect their PII.

B. Despite Its Promises, T-Mobile Failed to Protective Sensitive PII

29. At the same time T-Mobile collected, stored, and profited from Plaintiff's PII—and was actively communicating to consumers that they can "trust" T-Mobile with their sensitive data—it suffered a massive data breach compromising the PII of millions of its customers.

30. On January 19, 2023, T-Mobile announced that a "bad actor" had compromised the PII of "approximately 37 million current postpaid and prepaid customer accounts."[11]

31. Although T-Mobile has released very little information about the Data Breach, it has stated that its customers PII was compromised through an "Application Programming Interface" or "API."[12]

32. APIs are "instructions that allow applications to access data and interact with web databases"[13] and, if "left improperly secured, these APIs can be leveraged by malicious actors to mass-harvest information stored in those databases."

33. Upon detection, T-Mobile stated that it "promptly commenced an investigation with external cybersecurity experts," and "within a day of learning of the malicious activity, we were able to trace the source of the malicious activity and stop it," asserting that "the malicious activity appears to be fully contained at this time."[14]

---

[11] *T-Mobile Informing Impacted Customers about Unauthorized Activity* (Jan. 19, 2023), available at https://www.t-mobile.com/news/business/customer-information; T-Mobile US, Inc. Current Report (Form 8-K) (Jan. 19, 2023), available at https://www.sec.gov/ix?doc=/Archives/edgar/data/0001283699/000119312523010949/d641142d8k.htm.

[12] *T-Mobile Informing Impacted Customers about Unauthorized Activity* (Jan. 19, 2023), available at https://www.t- mobile.com/news/business/customer-information; T-Mobile US, Inc. Current Report (Form 8-K) (Jan. 19, 2023), available at T-Mobile US, Inc. Current Report (Form 8-K) (Jan. 19, 2023), available at https://www.sec.gov/ix?doc=/Archives/edgar/data/0001283699/000119312523010949/d641142d8k.htm.

[13] *New T-Mobile Breach Affects 37 Million Accounts* (Jan. 19, 2023), available at https://krebsonsecurity.com/2023/01/new-t-mobile-breach-affects-37-million-accounts/.

[14] *T-Mobile Informing Impacted Customers about Unauthorized Activity* (Jan. 19, 2023

34. T-Mobile further revealed that it believes "the bad actor first retrieved data through the impacted API starting on or around November 25, 2022," and that it failed to detect the unauthorized activity until January 5, 2023.[15]

35. Jake Williams, an incident responder and analyst at the Institute for Applied Network Security, stated that "the bottom line" is that T-Mobile's failure to detect the Data Breach for approximately six weeks indicates that "T-Mobile's API security clearly needs work"—it "shouldn't be having mass API abuse for more than six weeks."[16]

36. Likewise, Chester Wisniewski, field chief technical officer of applied research at the security firm Sophos, opined that it is "concerning that the criminals were in T-Mobile's system for more than a month before being discovered," and this "suggests T-Mobile's defenses do not utilize modern security monitoring and threat hunting teams, as you might expect to find in a large enterprise like a mobile network operator."[17]

37. The categories of PII compromised in the Data Breach include but are not limited to "name, billing address, email, phone number, date of birth, account number, and information such as the number of lines on the account and service plan features."[18]

C. T-Mobile Compounded Its Failure By Providing Inadequate Notice.

[15] Id.

[16] *T-Mobile's $150 Million Security Plan Isn't Cutting It* (Jan. 28, 2023), available at https://www.wired.com/story/tmobile-data-breach-again/

[17] Id.

[18] T-Mobile Informing Impacted Customers about Unauthorized Activity (Jan. 19, 2023), available at https://www.t-mobile.com/news/business/customer-information; T-Mobile US, Inc. Current Report (Form 8-K) (Jan. 19, 2023), available at https://www.sec.gov/ix?doc=/Archives/edgar/

38. T-Mobile has stated that it has "notified certain federal agencies about the incident" and has "begun notifying customers whose information may have been obtained by the bad actor in accordance with applicable state and federal requirements."[19]

39. However, notices sent to and received by victims of the Data Breach are woefully deficient. Instead of warning Data Breach victims that they are significant risk of identity theft and fraud, a notice by T-Mobile states that T-Mobile "prevented the most sensitive types of customer information from being accessed," and that "[c]ustomer accounts and finances are not put directly at risk by this event."[20]

40. Similarly, a notice received by Plaintiff states that T-Mobile's "systems and policies prevented the most sensitive types of customer information from being accessed," and "[c]ustomer accounts and finances are not directly at risk from this event."[21]

41. Likewise, in its press release, T-Mobile "tried to downplay the value of what was stolen," stating that it believed "[n]o passwords, payment card information, social security numbers, government ID numbers or other financial account information were compromised" and asserting that "no information was obtained for impacted customers that would compromise the safety of customer accounts or finances," and that "customer accounts and finances should not be put at risk directly by this event."[22]

---

[19] *T-Mobile Informing Impacted Customers about Unauthorized Activity* (Jan. 19, 2023), available at https://www.t- mobile.com/news/business/customer-information.

[20] *T-Mobile Informing Impacted Customers about Unauthorized Activity* (Jan. 19, 2023), available at https://www.t- mobile.com/news/business/customer-information.

[21] Id.

[22] *T-Mobile Informing Impacted Customers about Unauthorized Activity* (Jan. 19, 2023), available at https://www.t- mobile.com/news/business/customer-information.

42. However, this is highly misleading as the PII compromised in the Data Breach significantly increases the risk of identity theft and fraud for victims. For example, Chester Wisniewski, field chief technical officer of applied research at the security firm Sophos, stated that "[t]he information stolen in this breach is ideal for SIM swapping attacks and other forms of identity theft," which "should be another reason for T-Mobile customers to lock down their accounts and move away from SMS-based multifactor authentication" for financial accounts.

43. Similarly, Justin Fier, senior vice president for red team operations at the security company Darktrace, stated that such a massive treasure trove of consumer profiles could be of use to everyone from nation-state hackers to criminal syndicates: "There are dozens of ways that the information that was stolen could be weaponized."[17] For instance, for victims of the Data Breach, "there's a bigger possibility they'll be targeted by scammers, possibly impersonating T-Mobile, either by phone or email," and [a]rmed with key tidbits of information like account numbers, those scammers will sound much more convincing."[18] Similarly, Data Breach victims are at risk of "SIM swapping attacks, where cybercriminals contact a wireless carrier and use stolen personal information to pass themselves off as an account holder," then "ask that their phone number be transferred to a new SIM card," which "could give them access to not only the wireless number and account, but also any two-factor authentication codes that might come to the phone via SMS."[19]

44. Likewise, data security researcher Brian Krebs stated that "if the past is any teacher much of [the compromised data] will wind up posted online soon," and "[i]t is a safe bet that scammers will use some of this information to target T-Mobile users with phishing messages, account takeovers and harassment."[20] For this reason, "T-Mobile customers should fully expect to see phishers taking advantage of public concern over the breach to impersonate the company—

and possibly even send messages that include the recipient's compromised account details to make the communications look more legitimate."[23]

45. Similarly, "[d]ata stolen and exposed in this breach may also be used for identity theft," including SIM-swap attacks, and because "[m]any online services allow users to reset their passwords just by clicking a link sent via SMS," mobile phone numbers have become "de facto identity documents," as a result of which "losing control over your phone number thanks to an unauthorized SIM swap" can have devastating" consequences.[24]

46. T-Mobile's efforts to notify Plaintiff and Class Members thus fell short of providing key information about the Data Breach, consisting of brief messages with little substantive information that failed to warn victims to take action to protect themselves from identity theft and fraud.

47. T-Mobile's deficient notices compounded the harm suffered by Plaintiff and Class Members, by failing to timely provide Breach victims with the very details necessary to protect themselves.

D. T-Mobile Has A Long History Of Repeated Data Breaches.

48. The Breach and resulting harm suffered by Plaintiff and Class Members is directly attributable to T-Mobile's history of security lapses and data mismanagement. Indeed, T-Mobile is no stranger to cybersecurity incidents resulting from its flawed security. Rather, data breaches have been a nearly annual event for the company for many years.

[23] *New T-Mobile Breach Affects 37 Million Accounts* (Jan. 19, 2023), available at https://krebsonsecurity.com/2023/01/new-t-mobile-breach-affects-37-million-accounts/.

[24] *T-Mobile Gets Hacked Again: Is the Un-Carrier Un-Safe?* (Jan. 21, 2023), available at https://www.cnet.com/

49. In 2017, Karan Saini, a security researcher, found a bug on a T-Mobile website that allowed hackers to access PII like email addresses, account numbers, and IMSI numbers, just by knowing or guessing a customer's phone number.[23]

50. According to Saini, "T-Mobile has 76 million customers, and an attacker could have ran a script to scrape the data (email, name, billing account number, IMSI number, other numbers under the same account which are usually family members) from all 76 million of these customers to create a searchable database with accurate and up-to-date information of all users."[24] Saini explained "[t]hat would effectively be classified as a very critical data breach, making every T-Mobile cell phone owner a victim."[25]

51. T-Mobile had no mechanism in place to prevent this type of critical data breach, according to Saini.[26]

52. According to a hacker, the bug had been exploited by multiple hackers over a multi-week period before it was discovered by Saini.[27] In fact, the hackers who found the bug before Saini went so far as to upload a tutorial on how to exploit it on YouTube.[28]

53. In 2018, hackers gained access to T-Mobile servers and stole the PII of roughly two million T-Mobile customers.[25] The stolen PII included names, email addresses, account numbers, other billing information, and encrypted passwords.[26] T-Mobile misleadingly downplayed the hack, claiming that no passwords were "compromised."[27]

54. In truth, the hackers stole millions of encrypted passwords that were likely decrypted by the hackers due to the weak encoding algorithm employed by T-Mobile, leading one

[25] Lorenzo Franceschi-Bicchierai, *Hackers Stole Personal Data of 2 Million T-Mobile Customers,* Motherboard (Aug, 23, 2018), available at https://www.vice.com/en/article/a3qpk5/t-mobile-hack-data-breach-api-customer- data.

[26] Id.

[27] Id.

security expert to advise affected customers to assume their passwords were cracked and change them as a result.

55. In November 2019, hackers accessed the PII of roughly 1 million T-Mobile prepaid customers.[28] The PII in that breach included names, phone numbers, addresses, account information, and rate, plan and calling features (i.e., paying for international calls).[34]

56. In March 2020, T-Mobile disclosed it was subject to a data breach that exposed customer and employee PII, including names, addresses, social security numbers, financial account information, government identification numbers, phone numbers and billing account information.

57. Later in 2020, T-Mobile suffered yet another data breach in which hackers accessed customer proprietary network information (CPNI) and undisclosed call-related information for hundreds of thousands of customers.[29]

58. In August 2021, reports emerged that T-Mobile had suffered one of the largest data breaches in history, in which one or more cybercriminals exploited T-Mobile's data security protocols and gained access to internal servers containing the PII of approximately 76.6 million current, former, and prospective T-Mobile customers—including names, addresses, dates of birth, driver's license numbers, Social Security Numbers, phone numbers, and unique technical identifiers tethered to customers' mobile phones—exfiltrating a purported 106 GB of this data and posting a subset of the stolen PII for sale on a dark-web forum.[30]

59. In December 2021, T-Mobile disclosed that several customers had experienced SIM-swap attacks, stating: "We informed a very small number of customers that the SIM card

[28] Devin Coldeway, *More Than 1 Million T-Mobile Customers Exposed by Breach*, TechCrunch (Nov. 22, 2019), available at https://techcrunch.com/2019/11/22/more-than-1-million-t-mobile-customers-exposed-by-breach/.
[29] Id.

assigned to a mobile number on their account may have been illegally reassigned or limited account information was viewed."[31]

60. Further, in April 2022 it was announced that members of the LAPSUS$ cybercrime group breached T-Mobile multiple times in March, stealing source code for a range of company projects and accessing employee accounts with access to Atlas, a powerful internal T-Mobile tool for managing customer accounts.

61. Given the numerous data breaches pre-dating the Breach at issue in this case, T-Mobile was clearly aware of its data security failures, and the fact that subsequent breaches have occurred reinforces that Plaintiff's PII, which remains in T-Mobile's possession, is not safe.

62. As Chester Wisniewski, field chief technical officer of applied research at the security firm Sophos, stated, "I'm certainly disappointed to hear that, after as many breaches as they've had, they still haven't been able to shore up their leaky ship," lamenting "[a]nother day, another T-Mobile breach."[32]

63. Similarly, Neil Mack, senior analyst for Moody's Investors Service, stated "[w]hile these cybersecurity breaches may not be systemic in nature, their frequency of occurrence at T-Mobile is an alarming outlier relative to telecom peers," noting that the latest breach raises serious questions about T-Mobile's management's cyber governance.[33]

E. T-Mobile Failed To Comply With Regulatory Guidance And Industry-Standard Cybersecurity Practices.

[31] *See, e.g., Hacker claims to steal data of 100 million T-mobile customers* (Aug. 15, 2021). available at https://www.bleepingcomputer.com/news/security/hacker-claims-to-steal-data-of-100-million-t-mobile- customers/; *T-Mobile Suffers Another Data Breach, Affecting 37 Million Accounts* (Jan. 19, 2023), available at https://www.cnet.com/tech/mobile/another-data-breach-has-hit-t-mobile-impacting-37-million-accounts/.

[32] *T-Mobile's $150 Million Security Plan Isn't Cutting It* (Jan. 28, 2023), available at https://www.wired.com/story/tmobile-data-breach-again/

[33] *In latest T-Mobile hack, 37 million customers have personal data stolen, company says* (Jan. 20, 2023), available at https://www.usatoday.com/story/tech/2023/01/20/tmobile-data-hack-37-million-customers/11088603002/.

64. T-Mobile's long and well-documented history of data security failures is attributable to its failure to comply with state and federal laws and requirements as well as industry standards governing the protection of PII.

65. For example, at least 24 states have enacted laws addressing data security practice that require that businesses that own, license or maintain PII to implement and maintain reasonable security procedures and practices and to protect PII from unauthorized access. South Carolina is one of these states, South Carolina requires a business to provide adequate notice of a security breach to its customers. See S.C. Code Ann. § 39-1-90. Also, South Carolina requires certain businesses, in regard to cybersecurity: "Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control, each licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment and that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system." See S.C. Code Ann. § 38-99-20.

66. T-Mobile also failed to comply with Federal Trade Commission ("FTC") guidance on protecting PII and industry-standard cybersecurity practices. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

67. The FTC recommends:

i. limiting access to customer information to employees who have a business reason to see it;

ii. keeping customer information in encrypted files provides better protection in case of theft;

iii. maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information;

iv. using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information;

v. monitoring both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and,

vi. monitoring activity logs for signs of unauthorized access to customer information.[34]

68. The FTC has also issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[35]

69. In 2016, the FTC updated its publication, Protecting PII: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[36] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

[34] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business
[35] Federal Trade Commission, *Start With Security* at 2, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[36] Federal Trade Commission, *Protecting PII: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

70. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

71. The FTC recommends that businesses delete payment card information after the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

72. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

73. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

74. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data.

75. T-Mobile was aware of its obligations to protect its customers' PII and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers' PII from unauthorized access.

76. In this case, T-Mobile was at all times fully aware of its obligation to protect the PII of its customers. T-Mobile was also aware of the significant repercussions if it failed to do so because T-Mobile collected PII from millions of consumers and it knew that this PII hacked, would result in injury to consumers, including Plaintiff and Class Members.

77. Based upon the known details of the Data Breach and how it occurred, T-Mobile also failed to fully comply with industry-standard cybersecurity practices, including, but not limited to, proper firewall configuration, network segmentation, secure credential storage, rate limiting, user-activity monitoring, data-loss prevention, and intrusion detection and prevention.

F. The Effect Of The Data Breach On Plaintiff and Class Members.

78. T-Mobile's failure to keep Plaintiff's and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach—including names, addresses, email addresses, phone numbers, dates of birth, account numbers, and other account information—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future.

79. As a result, Plaintiff has suffered injury and faces an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

80. Further, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victim of several cybercrimes stemming from a single data breach.

81. Moreover, although elements of some Plaintiff's and Class Members' data may have been compromised in other data breaches, the fact that the Data Breach centralizes the PII

and identifies the victims as T-Mobile's customers materially increases the risk to Plaintiff and the Class.

82. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[37]

83. Moreover, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. Plaintiff will therefore need to spend time and money to continuously monitor her accounts for years to ensure her PII obtained in the Data Breach is not used to harm her. Plaintiff and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach. In other words, Plaintiff has been harmed by the value of identity protection services she must purchase in the future to ameliorate the risk of harm she now faces due to the Breach.

84. Plaintiff and Class Members have also realized harm in the lost or reduced value of their PII. T-Mobile admits the PII compromised in the Breach is valuable. As discussed above, T-Mobile collects, retains, and uses Plaintiff's PII to increase profits through predictive and other targeted marketing campaigns. Plaintiff's PII is not only valuable to T-Mobile, but Plaintiff also places value on her PII based on her understanding that her PII is a financial asset to companies that collect it.[38]

---

[38] *See, e.g., Ponemon Institute, LLC, Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers* at p. 14 (March 2015) (explaining that 53% of respondents "believe personal data is a financial asset similar to traded goods, currencies or commodities" and valuing, as but one example, their Social Security number at $55.70), available at https://docplayer.net/836701-Privacy-and-security-in-a-connected-life-a-study-of-us-european-and-japanese-consumers.html.

85. Plaintiff and Class Members have also been harmed and damaged in the amount of the market value of the hacker's access to Plaintiff's PII that was permitted without authorization by T-Mobile. This market value for access to PII can be determined by reference to both legitimate and illegitimate markets for such information.

86. Moreover, Plaintiff and Class Members value the privacy of this information and expect T-Mobile to allocate enough resources to ensure it is adequately protected. Customers would not have done business with T-Mobile, provided their PII and payment card information, or paid the same prices for T-Mobile's goods and services had they known T-Mobile did not implement reasonable security measures to protect their PII Customers reasonably expect that the payments they make to the carrier, either prepaid or each month, incorporate the costs to implement reasonable security measures to protect customers' PII. And because consumers value data privacy and security, companies with robust data security practices can command higher prices than those who do not. As a result, Plaintiff and Class Members did not receive the benefit of their bargain with T-Mobile because they paid a value for services they expected but did not receive.

87. Plaintiff and Class Members are also at risk of a harm specific to this Data Breach—"SIM swap" fraud. A SIM swap is a scheme wherein a hacker gains control of a victim's mobile phone number and service in order to intercept communications, including text messages, intended for the victim. The hackers then use that phone number as a key to access and take over the victim's other digital accounts, such as email, file storage, and financial accounts.

88. Customers often request SIM swaps for legitimate reasons when they obtain new phones or switch mobile carriers. However, T-Mobile does not have adequate protections in place to prevent fraudulent SIM swap attacks from occurring, and the data released in the Data Breach makes it much more likely that a T-Mobile customer will become a victim of a SIM swap attack.

In a fraudulent SIM swap, a would-be hacker contacts T-Mobile and impersonates the legitimate customer. This impersonation is made substantially easier when directed at T-Mobile customers, because hackers now have access to troves of data about T-Mobile customers, including their full names, addresses, email addresses, telephone numbers, and other data.

89. Following a fraudulent SIM swap (1) the legitimate subscriber (now victim)'s phone loses connection to the wireless network, meaning they cannot use the wireless network to call, text, or use the internet, and they are inhibited in their attempts to warn their wireless carrier of the fraud; and (2) all phone calls and text messages that would normally have gone to the victim's phone now go to the imposter's phone. If the imposter has even one other data point, such as an email address, he can often use the phone number to get into the victim's email account through the "Forgotten Password" feature, or by using the victim's legitimate phone number to pass two-factor authentication. Because customer email addresses were compromised in the Breach (and connected to a T-Mobile customer), this data is now readily available to would-be SIM swap hackers.

90. Given T-Mobile's failure to protect Plaintiff's and the Class Members' PII despite multiple data breaches in the past as well as subsequent data breaches, Plaintiff has a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages, restitution, or disgorgement) that protects her from suffering further harm, as her PII remains in T-Mobile's possession. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

91. In sum, Plaintiff and Class Members were injured as follows: (i) theft of their PII and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII;

(iii) loss of value of their PII; (iv) the lost value of access to Plaintiff's and Class Members' PII permitted by T-Mobile; (v) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; (vi) T-Mobile's retention of profits attributable to Plaintiff's and Class Members' PII that T-Mobile failed to adequately protect; (vii) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (viii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (ix) overpayments to T-Mobile for goods and services purchased, as Plaintiff reasonably believed a portion of the sale price would fund reasonable security measures that would protect her PII, which was not the case; and (x) nominal damages.

V. CLASS ALLEGATIONS

a. NATIONWIDE CLASS

92. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of the following nationwide class (the "Nationwide Class" or the "Class"):

All natural persons residing in the United States whose PII was exfiltrated in the Data Breach.

93. The Nationwide Class asserts claims against T-Mobile for negligence (Count 1), negligence per se (Count 2), breach of confidence (Count 3), intrusion upon seclusion (Count 4), breach of express contract (Count 5), breach of implied contract (Count 6), unjust enrichment (Count 7), and declaratory judgment (Count 8).

b. South Carolina Subclass

94. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of a South Carolina Subclass in the alternative to the nationwide claims (Counts

1 through 8), as well as with respect to statutory claims under South Carolina Code Ann. § 39-1-90 and Invasion of Privacy under South Carolina Common Law, on behalf of a South Carolina Subclass, defined as follows:

All natural persons residing in South Carolina whose PII was exfiltrated in the Data Breach.

95. Excluded from the Nationwide Class and the South Carolina Subclass (collectively, the "Class") are T-Mobile, any entity in which T-Mobile has a controlling interest, and T-Mobile's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

96. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of the Nationwide Class and the South Carolina Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, T-Mobile has acknowledged that millions of individuals' PII has been compromised. Those individuals' names and addresses are available from T-Mobile's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least thousands of individuals in the Nationwide Class and at least thousands of individuals in the South Carolina Statewide Subclass, making joinder of all Class Members impracticable.

97. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** As to both the Nationwide Class and the South Carolina Subclass, this action involves common questions of law and fact, which predominate over any questions affecting individual Class Members. The common questions include:

a. Whether T-Mobile had a duty to protect PII;

b. Whether T-Mobile failed to take reasonable and prudent security measures to ensure its systems were protected;

c. Whether T-Mobile failed to take available steps to prevent and stop the Breach from happening;

d. Whether T-Mobile knew or should have known that its computer and data storage systems were vulnerable to attack;

e. Whether T-Mobile was negligent in failing to implement reasonable and adequate security procedures and practices;

f. Whether T-Mobile's security measures to protect its systems were reasonable in light known legal requirements;

g. Whether T-Mobile's conduct constituted unfair or deceptive trade practices';

h. Whether T-Mobile violated state or federal law when it failed to implement reasonable security procedures and practices;

i. Which security procedures and notification procedures T-Mobile should be required to implement;

j. Whether T-Mobile has a contractual obligation to provide for the security of customer PII;

k. Whether T-Mobile has complied with any contractual obligations to protect customer PII;

l. What security measures, if any, must be implemented by T-Mobile to comply with its contractual obligations;

m. Whether T-Mobile violated state consumer protection laws in connection with the actions described herein;

n. Whether T-Mobile failed to notify Plaintiff and Class Members as soon as practicable and without delay after the Data Breach was discovered;

o. Whether T-Mobile's conduct resulted in or was the proximate cause of the loss of the PII of Plaintiff and Class Members;

p. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of T-Mobile's failure to reasonably protect their PII;

q. Whether T-Mobile should retain the money paid by Plaintiff and Class Members to protect their PII, and the profits T-Mobile generated using Plaintiff's and Class Members' PII;

r. Whether T-Mobile should retain Plaintiff's and Class Members' valuable PII; and,

s. Whether Plaintiff and Class Members are entitled to damages or injunctive relief.

98. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** As to the Nationwide Class and the South Carolina Subclass, Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way. Plaintiff's PII was in T-Mobile's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to those of other Class Members and Plaintiff seeks relief consistent with the relief of the Class.

99. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Nationwide Class and the South Carolina Subclass because Plaintiff is a member of the Nationwide Class and the South Carolina Subclass and is committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy

litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

100. **Predominance & Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against T-Mobile, and thus, individual litigation to redress T-Mobile's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court

101. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for T-Mobile or would be dispositive of the interests of members of the proposed Class.

102. **Ascertainability.** The Nationwide Class and South Carolina Subclass are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who

fits within the Class. The Nationwide Class and South Carolina Subclass consist of individuals who provided their PII to T-Mobile. Class Membership can be determined using T-Mobile's records.

103. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

104. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT ONE: NEGLIGENCE
(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE SOUTH CAROLINA SUBCLASS)

105. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

106. T-Mobile required Plaintiff and Class Members to submit sensitive PII in order to obtain or apply for its products and services.

107. T-Mobile owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons.

108. More specifically, this duty included, among other things: (a) designing, maintaining, and testing T-Mobile's security systems to ensure that Plaintiff's and Class Members' PII in T-Mobile's possession was adequately secured and protected; (b) implementing processes that would

detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

109. T-Mobile's duty to use reasonable care arose from several sources, including but not limited to those described herein.

110. T-Mobile had common law duties to prevent foreseeable harm to Plaintiff and the Class Members. These duties existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiff and Class Members would be harmed by T-Mobile's failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, T-Mobile knew that it was more likely than not Plaintiff and other Class Members would be harmed if it allowed such a breach.

111. T-Mobile's duty to use reasonable security measures also arose as a result of the special relationship that existed between T-Mobile, on the one hand, and Plaintiff and Class Members, on the other hand. The special relationship arose because Plaintiff and Class Members entrusted T-Mobile with their PII as part of the applications for or purchase and signing-up for the products and services T-Mobile offers as a major telecommunications company. T-Mobile alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

112. T-Mobile's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies such as T-Mobile. Various FTC publications and data security

breach orders further form the basis of T-Mobile's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

113. T-Mobile's duty also arose from T-Mobile's unique position as the second largest wireless carrier in the United States. As a telecommunications company, T-Mobile holds itself out as a protector of consumer data, and thereby assumes a duty to reasonably protect the data that was provided to it by Plaintiff and Class Members. T-Mobile has stated that consumers "trust T-Mobile to connect you to the world every day, and we're working hard to earn a place in your heart. A big part of that is maintaining your privacy."[39] Because of its role as the second largest wireless carrier, T-Mobile was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the T-Mobile Data Breach.

114. T-Mobile admits that it has a responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the PII at issue here.

115. With regard to network security, T-Mobile further acknowledges that it "use[s] administrative, technical, contractual, and physical safeguards designed to protect your data."[40]

116. T-Mobile knew or should have known that its computing systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII.

117. T-Mobile also had a duty to safeguard the PII of Plaintiff and Class Members and to promptly notify them of a breach because of state laws and statutes that require T-Mobile to reasonably safeguard sensitive PII, as detailed herein.

118. Timely, adequate notification was required, appropriate and necessary so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or lock their

[39] https://www.t-mobile.com/privacy-center/privacy-notices/t-mobile-privacy-notice
[40] Id.

credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by T-Mobile's misconduct.

119. T-Mobile breached the duties it owed to Plaintiff and Class Members described above and thus was negligent. T-Mobile breached these duties by, among other things, failing to:

a. exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members;

b. detect the Breach while it was ongoing;

c. maintain security systems consistent with industry standards during the period of the Data Breach;

d. comply with regulations protecting the PII at issue during the period of the Data Breach; and

e. disclose in a timely and adequate manner that Plaintiff's and the Class Members' PII in T-Mobile's possession had been or was reasonably believed to have been, stolen or compromised.

120. But for T-Mobile's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

121. T-Mobile's failure to take proper security measures to protect the sensitive PII of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiff's and Class Members' PII.

122. Plaintiff and Class Members were foreseeable victims of T-Mobile's inadequate data security practices, and it was also foreseeable that T-Mobile's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiff and Class Members as described in this Complaint.

123. As a direct and proximate result of T-Mobile's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages and other economic and non-economic harm.

COUNT TWO: NEGLIGENCE PER SE
(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE SOUTH CAROLINA SUBCLASS)

124. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

125. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as T-Mobile of failing to use reasonable measures to protect PII.

126. The FTC publications and orders also form the basis of T-Mobile's duty.

127. T-Mobile violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. T-Mobile's conduct was particularly unreasonable given the nature and amount of PII it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving a company as large as T-Mobile, including, specifically the damages that would result to Plaintiff and Class Members.

128. In addition, under state data security statutes, T-Mobile had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' PII.

129. T-Mobile's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

130. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

131. The harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

132. T-Mobile breached its duties to Plaintiff and Class Members under the FTC Act and state data security statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

133. Plaintiff and Class Members were foreseeable victims of T-Mobile's violations of the FTC Act and state data security statutes. T-Mobile knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiff's and Class Members' PII would cause damage to Plaintiff and Class Members.

134. But for T-Mobile's violation of the applicable laws and regulations, Plaintiff's and Class Members' PII would not have been accessed by unauthorized parties.

135. As a direct and proximate result of T-Mobile's negligence per se, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and

overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT THREE: BREACH OF CONFIDENCE
(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE SOUTH CAROLINA SUBCLASS)

136. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

137. Plaintiff and Class Members maintained a confidential relationship with T-Mobile whereby T-Mobile undertook a duty not to disclose to unauthorized parties the PII provided by Plaintiff and Class Members to T-Mobile to unauthorized third parties. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

138. T-Mobile knew Plaintiff's and Class Members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII they collected, stored, and maintained.

139. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiff's and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred because T-Mobile failed to implement and maintain reasonable safeguards to protect the PII in its possession and failed to comply with industry-standard data security practices.

140. Plaintiff and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

141. But for T-Mobile's disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen,

viewed, accessed, and used by unauthorized third parties. T-Mobile's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

142. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of T-Mobile's unauthorized disclosure of Plaintiff's and Class Members' PII. T-Mobile knew its computer systems and technologies for accepting, securing, and storing Plaintiff's and Class Members' PII had serious security vulnerabilities because T-Mobile failed to observe even basic information security practices or correct known security vulnerabilities.

143. As a direct and proximate result of T-Mobile's breach of confidence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm

COUNT FOUR: INVASION OF PRIVACY

(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE SOUTH CAROLINA SUBCLASS)

144. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

145. Plaintiff shared PII with T-Mobile that Plaintiff wanted to remain private and non-public.

146. Plaintiff reasonably expected that the PII Plaintiff shared with T-Mobile would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

147. T-Mobile intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party.

148. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, T-Mobile unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII properly obtained for specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

149. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial and other PII.

150. T-Mobile's intrusions into Plaintiff's and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

151. As a direct and proximate result of T-Mobile's invasions of privacy, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT FIVE: BREACH OF EXPRESS CONTRACT
(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE SOUTH CAROLINA SUBCLASS)

152. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

153. T-Mobile's Privacy Notice is an agreement between T-Mobile and individuals who provided their PII to T-Mobile, including Plaintiff and Class Members.

154. T-Mobile's Privacy Notice states that it applies "to personal data we have about you," meaning "data that identifies, relates to, describes, can be associated with, or could reasonably identify you as an individual." This includes "data like your name, address, or email address, as well as less obvious data like demographic data, device and usage data, call records, advertising ID, and location data[.]" It further states that the Notice applies to "all personal data we collect and use when you access or use our cell and data services, websites, apps, and other services (our 'services'), purchase and use our devices and products ('products'), visit our retail stores, or communicate or interact with us in any way."

155. T-Mobile's Privacy Notice stated at the time of the Data Breach that T-Mobile "use[s] administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control."[41]

156. T-Mobile further agreed at the time of the Data Breach that it would only share data under certain enumerated circumstances, which include: "with your consent or at your direction," "with the account holder," "between T-Mobile brands and companies," "to provide benefits," "to our service providers," "to other third parties . . . for uses described in this notice or for purposes you have requested," "for identity verification and fraud prevention services," "caller ID providers," "in a business transfer or transaction" which is specified as a "corporate business transaction like an acquisition, divestiture, sale of company assets," and "for legal process and protection."[42] None of the enumerated circumstances involve sharing Plaintiff's or the Class Members' PII with a criminal hacker.

157. T-Mobile's emphasized in its Privacy Policy at the time of the Data Breach that those who provide their PII to T-Mobile "trust T-Mobile to connect you to the world every day, and we're

[41] https://www.t-mobile.com/privacy-center/privacy-notices/t-mobile-privacy-notice
[42] https://www.t-mobile.com/privacy-center/privacy-notices/t-mobile-privacy-notice

working hard to earn a place in your heart. A big part of that is maintaining your privacy. We believe you deserve transparency, education, choice, protection, and simplicity."[43] Plaintiff and Class Members on the one side and T-Mobile on the other formed a contract when Plaintiff and Class Members obtained products or services from T-Mobile, or otherwise provided PII to T-Mobile subject to its Privacy Policy.

158. Plaintiff and Class Members fully performed their obligations under the contracts with T-Mobile.

159. T-Mobile breached its agreement with Plaintiff and Class Members by failing to protect their PII. Specifically, it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

160. As a direct and proximate result of T-Mobile's breach of contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

161. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the

[43] Id.

amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT SIX: BREACH OF IMPLIED CONTRACT
(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE SOUTH CAROLINA SUBCLASS)

162. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

163. Plaintiff and Class Members entered into an implied contract with T-Mobile when they obtained products or services from T-Mobile, or otherwise provided PII to T-Mobile.

164. As part of these transactions, T-Mobile agreed to safeguard and protect the PII of Plaintiff and Class Members and to timely and accurately notify them if their PII was breached or compromised.

165. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that T-Mobile's data security practices and policies were reasonable and consistent with legal requirements and industry standards. Plaintiff and Class Members believed that T-Mobile would use part of the monies paid to T-Mobile under the implied contracts or the monies obtained from the benefits derived from the PII they provided to fund adequate and reasonable data security practices.

166. Plaintiff and Class Members would not have provided and entrusted their PII to T-Mobile or would have paid less for T-Mobile products or services in the absence of the implied contract or implied terms between them and T-Mobile. The safeguarding of the PII of Plaintiff and Class Members was critical to realize the intent of the parties.

167. Plaintiff and Class Members fully performed their obligations under the implied contracts with T-Mobile.

168. T-Mobile breached its implied contracts with Plaintiff and Class Members to protect their PII when it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties.

169. As a direct and proximate result of T-Mobile's breach of implied contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT SEVEN: UNJUST ENRICHMENT
(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE SOUTH CAROLINA SUBCLASS)

170. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

171. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by T-Mobile and that was ultimately stolen in the T-Mobile Data Breach.

172. T-Mobile was benefitted by the conferral upon it of the PII pertaining to Plaintiff and Class Members and by its ability to retain, use, sell, and profit from that information. T-Mobile understood that it was in fact so benefitted.

173. T-Mobile also understood and appreciated that the PII pertaining to Plaintiff and Class Members was private and confidential and its value depended upon T-Mobile maintaining the privacy and confidentiality of that PII.

174. But for T-Mobile's willingness and commitment to maintain its privacy and confidentiality, that PII would not have been transferred to and entrusted with T-Mobile.

175. T-Mobile admits that it uses the PII it collects for, among other things, advertising and marketing "products and services from T-Mobile and other companies to you, including through targeted advertising and communications about promotions and events, contents, and sweepstakes," and conducting research and creating reports "from analysis of things like usage patterns and trends and to deidentify or aggregate personal data to create business and market analysis and reports."[44]

176. Because of its use of Plaintiff's and Class Members' PII, T-Mobile sold more services and products than it otherwise would have. T-Mobile was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create to the detriment of Plaintiff and Class Members.

[44] https://www.t-mobile.com/privacy-center/privacy-notices/t-mobile-privacy-notice

177. T-Mobile also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiff's and Class Members' PII.

178. T-Mobile also benefitted through its unjust conduct in the form of the profits it gained through the use of Plaintiff's and Class Members' PII.

179. It is inequitable for T-Mobile to retain these benefits.

180. As a result of T-Mobile's wrongful conduct as alleged in this Complaint (including among things its failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiff and Class Members without having adequate data security measures, and its other conduct facilitating the theft of that PII), T-Mobile has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

181. T-Mobile's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class Members' sensitive PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

182. It is inequitable, unfair, and unjust for T-Mobile to retain these wrongfully obtained benefits. T-Mobile's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

183. The benefit conferred upon, received, and enjoyed by T-Mobile was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for T-Mobile to retain the benefit.

184. T-Mobile's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiff and Class Members to unfairly incur substantial time and/or costs to mitigate

and monitor the use of their PII and has caused the Plaintiff and Class Members other damages as described herein.

185. Plaintiff and the Class Members have no adequate remedy at law.

186. T-Mobile is therefore liable to Plaintiff and Class Members for restitution or disgorgement in the amount of the benefit conferred on T-Mobile as a result of its wrongful conduct, including specifically: the value to T-Mobile of the PII that was stolen in the Data Breach; the profits T-Mobile received and is receiving from the use of that information; the amounts that T-Mobile overcharged Plaintiff and Class Members for use of T-Mobile's products and services; and the amounts that T-Mobile should have spent to provide reasonable and adequate data security to protect Plaintiff's and Class Members' PII.

COUNT EIGHT: VIOLATION 28 U.S.C. §§2201 et seq., DECLARATORY JUDGEMENT (ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE SOUTH CAROLINA SUBCLASS)

187. Plaintiff repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

188. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

189. An actual controversy has arisen in the wake of the T-Mobile Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether T-Mobile is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff continues to suffer injury as a result of the compromise of Plaintiff's PII and remain at imminent risk that further

compromises of her PII will occur in the future given the publicity around the Data Breach and the nature and quantity of the PII stored by T-Mobile.

190. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. T-Mobile continues to owe a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. T-Mobile continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

191. The Court also should issue corresponding prospective injunctive relief requiring T-Mobile to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

192. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at T-Mobile. The risk of another such breach is real, immediate, and substantial. If another breach at T-Mobile occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and Plaintiff will be forced to bring multiple lawsuits to rectify the same conduct.

193. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to T-Mobile if an injunction is issued. Among other things, if another massive data breach occurs at T-Mobile, Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to T-Mobile of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and T-Mobile has a pre-existing legal obligation to employ such measures.

194. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at T-Mobile, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

COUNT NINE: VIOLATION OF S.C. CODE ANN. § 39-1-90

(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE SOUTH CAROLINA SUBCLASS)

195. The South Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeats and realleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

196. Defendant T-Mobile is a business that owns and possesses data as described by S.C. CODE § 39-1-90 (A).

197. Defendant T-Mobile was breached, as Defined by § 39-1-90 (D)(1): ""Breach of the security of the system" means unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident."

198. Pursuant to §39-1-90(B), :"A person conducting business in this State and maintaining computerized data or other data that includes personal identifying information that the person does not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person."

199. Defendant T-Mobile violated § 39-1-90 as it did not provide immediate notice.

200. Pursuant to Subsection G of § 39-1-90: "A resident of this State who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may:

a. institute a civil action to recover damages in case of a willful and knowing violation;

b. institute a civil action that must be limited to actual damages resulting from a violation in case of a negligent violation of this section;

c. seek an injunction to enforce compliance; and

d. recover attorney's fees and court costs, if successful.

201. Defendant T-Mobile knew, or should have known, that its systems were susceptible to breach accordingly, Defendant T-Mobile's systems were breached.

202. Upon this breach, and T-Mobile's notice of such breach, T-Mobile should have immediately notified its customers.

203. T-Mobile did not immediately notify its customers, and thus violated §39-1-90.

204. Plaintiff and South Carolina Subclass Members seek relief under § 39-1-90, including a civil fine, a recovery of such damages, an injunction, and attorney's fees.

COUNT TEN: VIOLATION OF PRIVACY: RIGHT TO PUBLICITY

(ON BEHALF OF THE NATIONWIDE CLASS, OR ALTERNATIVELY, ON BEHALF OF PLAINTIFF AND THE SOUTH CAROLINA SUBCLASS)

205. Under South Carolina common law, a person has a right to publicize and profit from use of their name, image, identity, images, and likeness.

206. Defendant T-Mobile acquired and has sold Plaintiff's and other Class Members' information including name, image, identity, images, and likeness without their consent.

207. Defendant received financial. compensation for such transfer of Plaintiff and Subclass Members. Defendant T-Mobile has not compensated Plaintiff or other Subclass Members for its use of their information including name, image, identity, images, and likeness.

208. Clearly, Defendant has violated Plaintiff's, and other South Carolina Subclass Members', right to publicity under well settled common law.

209. Under South Carolina law, there is a presumption of nominal damages in similar cases involving the infringement on the right to control the use of one's identity.

210. Plaintiffs are entitled to adequate compensation relative to the commercial value of their information.

VI. REQUEST FOR RELIEF

211. Plaintiff, individually and on behalf of members of the Nationwide Class and South Carolina Subclass, as applicable, respectfully requests that the Court enter judgment in Plaintiff's favor and against T-Mobile, as follows:

212. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

213. That the Court grant permanent injunctive relief to prohibit T-Mobile from continuing to engage in the unlawful acts, omissions, and practices described herein, including;

a. Prohibiting T-Mobile from engaging in the wrongful and unlawful acts described herein;

b. Requiring T-Mobile to protect all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. Requiring T-Mobile to delete, destroy and purge the PII of Plaintiff and Class Members unless T-Mobile can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. Requiring T-Mobile to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

e. Requiring T-Mobile to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on T-Mobile's systems on a periodic basis, and ordering T-Mobile to promptly correct any problems or issues detected by such third-party security auditors;

f. Requiring T-Mobile to engage independent third-party security auditors and internal personnel to run automated security monitoring;

g. Requiring T-Mobile to audit, test, and train its security personnel regarding any new or modified procedures; Requiring T-Mobile to segment data by, among other things, creating firewalls and access controls so that if one area of T-Mobile's network is compromised, hackers cannot gain access to other portions of T-Mobile's systems;

h. Requiring T-Mobile to conduct regular database scanning and securing checks;

i. Requiring T-Mobile to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective

responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

j. Requiring T-Mobile to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

k. Requiring T-Mobile to implement a system of testing to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with T-Mobile's policies, programs and systems for protecting PII;

l. Requiring T-Mobile to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor T-Mobile's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

m. Requiring T-Mobile to meaningfully educate all Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;

n. Requiring T-Mobile to implement logging and monitoring programs sufficient to track traffic to and from T-Mobile servers; and

o. Appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis T-Mobile's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment.

214. That the Court award Plaintiff and Class and Subclass Members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

215. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by T-Mobile as a result of its unlawful acts, omissions, and practices;

216. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

217. That Plaintiff be granted the declaratory relief sought herein;

218. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

219. That the Court award pre- and post-judgment interest at the maximum legal rate; and

220. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: January 31, 2023

By: */s/Paul J. Doolittle*
POULIN | WILLEY | ANASTOPOULO, LLC
Blake G. Abbott (Federal I.D. #13354)
Paul J. Doolittle (Federal I.D. #6012)
32 Ann Street

Charleston, SC 29403
Tel: (843) 614-8888
Email: blake@akimlawfirm.com
pauld@akimlawfirm.com